

## NOTE D'INFORMATION N°44/2020

La Défense, le 21 décembre 2020

**Objet : Campagne d'hameçonnage (ou phishing)**

**Important – merci de prendre le temps de lire cette note !**

Les **cyberattaques (ransomwares, malwares, phishing et autres virus)** sont des agressions extérieures qu'il est possible de bloquer avec un pare-feu et un proxy qui protègent les connexions web. Notre cybersécurité **informatique** passe par la **protection du réseau local mis en place par Flowline. Cependant avec le développement** du télétravail que nous connaissons, vous utilisez votre réseau personnel qui n'est pas autant sécurisé que le réseau Flowline.

Pour répondre au risque croissant de cyberfraude en entreprise et au contexte de télétravail qui augmente ce risque, le Comité de Direction a décidé en réunion du 27 novembre dernier de mettre en place une campagne d'hameçonnage.

La campagne d'hameçonnage a été menée entre le 17 et le 22 décembre 2020 sur les adresses mails professionnelles de tous les collaborateurs GSA+. Vous avez tous reçu un mail provenant de Gaëlle Bontet envoyé par les équipes de Flowline.

L'objectif de cette campagne est triple :

- Phase 1 :  
Lancement de la campagne et identification du risque  
Récolte des retours, analyse des données et identification de la population à risque.
- Phase 2 :  
Sensibilisation et formation des collaborateurs au repérage et à l'identification de l'hameçonnage.
- Phase 3 :  
Procédure d'action à réaliser à la suite d'hameçonnage d'un collaborateur

### Phase 1 : Identification du risque et analyse des retours

Tous les collaborateurs ont reçu un mail d'hameçonnage envoyé par les équipes de Flowline et provenant de Gaëlle Bontet.

**Les résultats de cette campagne sont les suivants :**

Sur les 41 mails envoyés, les résultats présentent un contexte à risque cyberfraude élevé ; 64% d'ouverture de lien et d'identification cumulées.

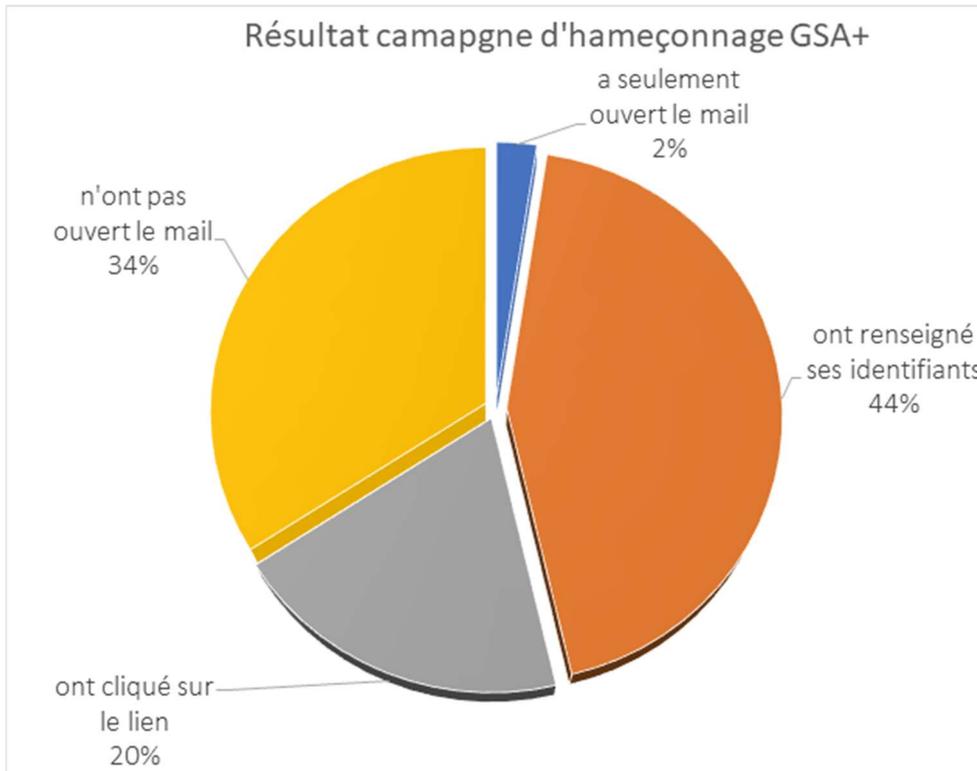
Cependant :

- Ce type d'hameçonnage ciblé est l'un des plus difficile à repérer (message non générique, population ciblée, carte de visite identique, charte graphique respectée).
- Beaucoup d'entre vous ont eu le bon réflexe d'informer Sophie Labry, Gaëlle Bontet ou leur correspondant informatique de ce mail « suspicieux ».

**C'est le 1<sup>er</sup> réflexe à avoir dans ce contexte.**

## Résultats :

- 14 personnes soit 34 % n'ont pas ouvert le mail : Bravo ! Aucun impact de la cyberfraude.
- 1 personne soit 2 % a ouvert le mail sans cliquer sur le lien : Bravo ! L'ouverture du mail n'implique généralement pas de risque.
- 8 personnes soit 20% ont ouvert le mail et cliqué sur le lien : il faut agir vite car le risque de cyberattaque est important (cf. Procédure)
- 18 personnes soit 44% ont ouvert le mail, cliqué sur le lien et se sont identifiées avec leur login / mot de passe : il faut agir vite car le risque de cyberattaque est important (cf. Procédure)



Vous trouverez ci-après, astuces et clés pour repérer un mail « frauduleux » ainsi que la procédure à respecter en cas d'hameçonnage.

## Phase 2 : sensibilisation et formation des collaborateurs au repérage et à l'identification de l'hameçonnage.

Prévenir le risque c'est nous former à le repérer.

Voici quelques clés pour identifier et éviter l'hameçonnage que nous vous demandons de lire attentivement.

### Il existe deux types d'hameçonnage :

- Hameçonnage générique :
  - Envoi mail aux hasards
  - Pas de personnalisation
  - En général assez facile à repérer
- Hameçonnage ciblé : Pratique de plus en plus utilisée
  - Population ciblée
  - Utilisation de notions mettant en confiance (noms connus, carte de visite mail utilisée, sujets habituels...)
  - Usurpation d'identité (une adresse correcte peut avoir été piratée)

## Ce qu'il faut vérifier pour éviter un hameçonnage : Astuces :

Ouvrir un mail n'est pas dangereux dans la plupart des cas,

Ce qui peut l'être c'est de cliquer sur un lien ou ouvrir une pièce jointe.

Il faut d'abord vérifier l'email (expéditeur, contenu, lien web, pièce jointe) avant toute action.

 <h3>Caractéristiques du phishing</h3> <ul style="list-style-type: none"><li>• Expéditeurs</li><li>• Liens</li><li>• Pièces jointes</li><li>• Contenu du mail</li></ul>	 <h3>Reconnaître l'expéditeur</h3> <ul style="list-style-type: none"><li>• Vérifier le nom de l'expéditeur</li><li>• Vérifier l'adresse en cliquant dessus</li><li>• En général le format doit être utilisateur@entreprise.fr ou .com</li></ul>	 <h3>Liens</h3> <ul style="list-style-type: none"><li>• De préférence ne pas cliquer sur un lien dans un mail</li><li>• Passer la souris dessus pour vérifier le chemin du mail</li><li>• Chercher sur un moteur de recherche pour atteindre le site en question</li></ul>	 <h3>Les pièces jointes</h3> <ul style="list-style-type: none"><li>• Redoubler de vigilance lorsque la pièce jointe contient un fichier avec une fin en .zip, .rar ou .exe</li><li>• Ne pas ouvrir si vous avez un doute sur l'expéditeur</li></ul>
--	--	--	--

## Dans un cas plus général voici comment détecter un hameçonnage :

- Le prénom est mal orthographié
- La partie du mail avant le @ ne correspond pas à l'identité
- Le nom de l'entreprise (après le @) n'est pas correct

- Via indique un relais, l'expéditeur n'envoie donc pas du serveur GSA+
- L'adresse après le via est suspecte car inconnue



Bonjour Jean-Wandrille,

Je viens de recevoir un mail des services de sécurité de la tour W.

Merci d'en prendre connaissance, ci-dessous le lien d'accès.

[Lien d'accès](#)

- Si vous connaissez bien l'expéditeur, demandez vous s'il s'exprime souvent ainsi. En cas de doute n'hésitez pas à l'appeler

Très bonnes fêtes de fin d'année !

Take care !

Bien cordialement,

**GSA+**  
Groupement de services assurances

Gaëlle Bontet  
Directeur GSA+  
01 47 76 53 55  
gaelle.bontet@gsaplus.fr  
Tour W - 102, terrasse Boieldieu - 92085 Paris La Défense cedex

- En plaçant la souris sur le lien, le chemin apparaît.
- L'adresse du chemin du lien indique un site « onlineservicetech.services... »
- Ce lien vous est inconnu, il est donc suspect. Ne cliquez pas

### Phase 3 : Définir une procédure d'action pour donner suite à hameçonnage d'un collaborateur

Vous avez été victime d'un hameçonnage, voici la procédure à suivre :

- a. Vous avez été hameçonné en cliquant sur un lien :

**Contactez immédiatement Sophie Labry ou Gaelle Bontet (administrateurs informatiques) et informez votre correspondant informatique (Delphine Guay, Michel Suin ou Clotilde Vautrin).**

Il est impératif de changer rapidement le mot de passe de votre session de travail de la manière suivante :

- Si vous êtes sur le site de la tour W :  
Vous pouvez le modifier en cliquant simultanément sur ctrl/alt/suppr – changer mot de passe
- Si vous êtes en télétravail :  
Vous devez contacter Sophie Labry ou Gaelle Bontet ou votre correspondant informatique afin d'ouvrir un ticket auprès du support Flowline pour le changement de mot votre mot de passe.

- b. Vous avez été hameçonné en ouvrant un fichier infecté :

**Contactez immédiatement Sophie Labry ou Gaelle Bontet (administrateurs informatiques) et informez votre correspondant informatique (Delphine Guay, Michel Suin ou Clotilde Vautrin).**

Il est indispensable de sortir rapidement du réseau pour ne pas infecter les autres collaborateurs.

- Si vous êtes sur le site de la tour W :  
**Débranchez IMMEDIATEMENT** votre ordinateur de la station d'accueil, **déconnectez** votre PC du **réseau wifi et éteignez votre ordinateur**
- Si vous êtes en télétravail :  
**Débranchez IMMEDIATEMENT** votre ordinateur du RDS et éteignez votre PC

Dans tous les cas, il est indispensable de prévenir Sophie Labry et/ou Gaëlle Bontet (administrateurs informatiques) afin de vérifier la sécurité du réseau et informer notre support technique dédié cybersécurité.

Les techniques de cyberfraude évoluent sans cesse, c'est pourquoi nous serons amenés à renouveler ces campagnes d'identification des risques et d'information régulièrement.

Nous vous remercions de votre vigilance.

Nous vous souhaitons de passer de bonnes fêtes de fin d'année.

Gaëlle BONTET  
Directeur



Diffusion Générale